Diese Anleitung soll dabei helfen, PGP unter Mac OS X mit dem Email-Client Thunderbird einzurichten. In dieser Anleitung wird nicht beschrieben, wie Thunderbird installiert oder eingerichtet wird. Dies gilt als Voraussetzung für eine erfolgreiche Installation und Konfiguration von PGP.
Für die Installation werden noch zwei weitere Programme benötigt:

- GPGTools https://github.com/downloads/GPGTools/GPGTools/GPGTools-20120318.dmg
- Thunderbird-Add-On „Enigmail“ https://addons.mozilla.org/thunderbird/downloads/latest/71/addon-71-latest.xpi?src=dp-btn-primary

Installation von GPGTools und Enigmail

Als Erstes muss die Software „GPGTools“ installiert werden. Nach erfolgreichem Download muss Apple Mail geschlossen werden und das dmg-Image (siehe Abbildung 1) geöffnet werden.

Abbildung 1: GPGTools Image

Nun wird die Installation mit Doppelklick auf das rotmarkierte Symbol gestartet. Klicken Sie nun „Fortfahren“ bis Sie zu der Ansicht in Abbildung 2 gelangen.

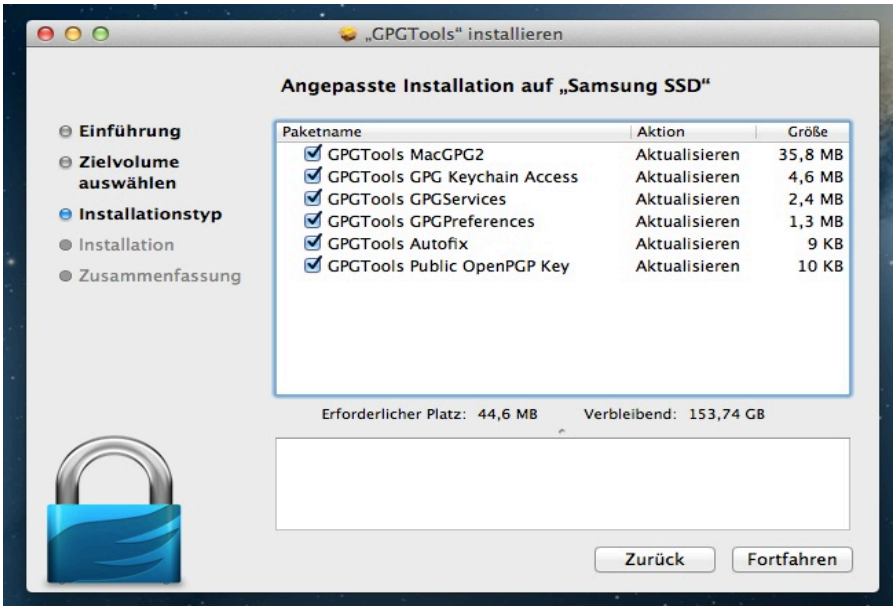

Abbildung 2: Installationsauswahl bei GPGTools

Wählen Sie die oben abgebildeten Einträge aus und klicken Sie auf „Fortfahren". In der nächsten Maske nur auf „Installieren" klicken und „GPGTools" wird installiert.

Nach Abschluss der Installation von „GPGTools" muss nun das Thunderbird-Add-On „Enigmail" installiert werden. Dazu öffnen Sie Thunderbird und klicken dort auf „Extras" und dann auf „Add-ons" (siehe Abbildung 3).

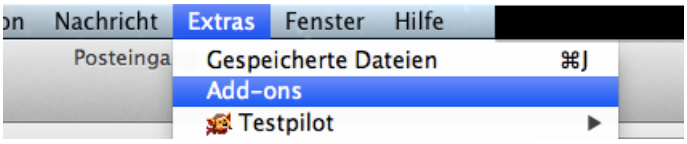

Abbildung 3: Add-ons Auswahl in Thunderbird

Klicken Sie dort auf das Zahnrädchen (siehe Abbildung 4) und dann auf „Add-on aus Datei installieren...". Suchen Sie nun die Datei „enigmail-1.5-tb+sm.xpi" in Ihrem Download-Ordner und drücken Sie „Öffnen". Im nächsten Fenster nur noch auf „Installieren" klicken und nach der Installation wird Thunderbird neugestartet.

Abbildung 4: Add-ons Einstellungen in Thundebird

Eigenen Schlüssel erstellen

Um einen eigenen Schlüssel zu erstellen, starten Sie das Programm „GPG Schlüsselbund". Dort klicken Sie in der Menüleiste auf „Schlüssel" und dann auf „Erstellen ..." (siehe Abbildung 5).

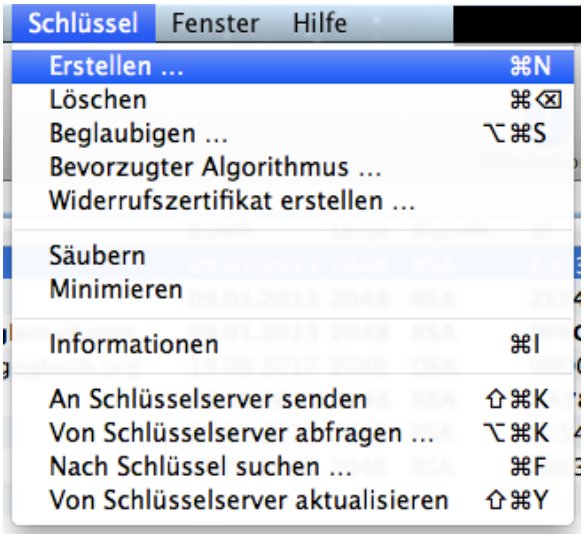

Abbildung 5: Eigenen PGP-Schlüssel erstellen

Im Fenster, welches sich jetzt öffnet, geben Sie Ihren vollständigen Namen sowie Ihre Email-Adresse, mit welcher Sie verschlüsselte Emails versenden möchten, ein. Möchten Sie Ihren öffentlichen Schlüssel direkt an einen Schlüsselserver senden, damit andere Personen Ihren öffentlichen Schlüssel von dort laden und Ihnen verschlüsselte Emails senden können, dann machen Sie einen Hacken bei „Upload key after generation“. Falls Sie Ihren Schlüssel nicht jetzt an den Schlüsselserver senden wollen, haben Sie die Möglichkeit dies später zu machen (siehe „Eigenen öffentlichen Schlüssel bereitstellen“).

Eigenen öffentlichen Schlüssel bereitstellen

Um Ihren öffentlichen Schlüssel an einen Schlüsselserver zu schicken, markieren Sie den Schlüssel und klicken dann in der Menüleiste auf „Schlüssel“ und auf „An Schlüsselserver senden“. Jetzt öffnet sich ein neues Fenster mit einem Ladenbalken und der Schlüssel wird versendet.

Öffentliche Schlüssel vom Schlüsselserver importieren

Sie haben die Möglichkeit auf dem Schlüsselserver nach öffentlichen Schlüsseln von anderen Personen zu suchen und diese zu importieren, um verschlüsselte Email an diese Personen zu schicken.
Dazu klicken Sie in der Menüleiste auf „Schlüssel“ und dann auf „Nach Schlüsseln suchen...“. Im neuen Fenster geben Sie den Namen der Person ein und drücken „Schlüssel suchen“. Nachdem die Schlüssel gefunden wurden, erscheint eine Auswahlliste mit möglichen Email-Adressen. Suchen Sie dort nach der passenden Email-Adresse, setzen den Hacken und drücken „Schlüssel holen“. Nun wird der Schlüssel importiert und Sie können der Person eine verschlüsselte Email senden.

Nachricht verschlüsseln und/oder signieren

Um nun eine verschlüsselte Nachricht an eine Person zu verschicken, benötigen Sie zum einen den öffentlichen Schlüssel (siehe „Öffentliche Schlüssel vom Schlüsselserver importieren“) sowie die Email-Adresse der Person. Besitzen Sie beides, öffnen Sie Thunderbird und drücken „Verfassen“. Geben Sie wie gewöhnlich die Email-Adresse, den Betreff und den Nachrichtentext ein. Wenn Sie die Email fertig verfasst haben, klicken Sie auf „OpenPGP“ (siehe Abbildung 6). Um die Email zu verschlüsseln, setzen Sie einen Hacken bei „Nachricht verschlüsseln“ (Grüne Markierung). Sie können

zusätzlich oder stattdessen die Nachricht auch noch signieren, dafür setzen Sie einen Hacken bei „Nachricht unterschreiben“ (Rote Markierung).

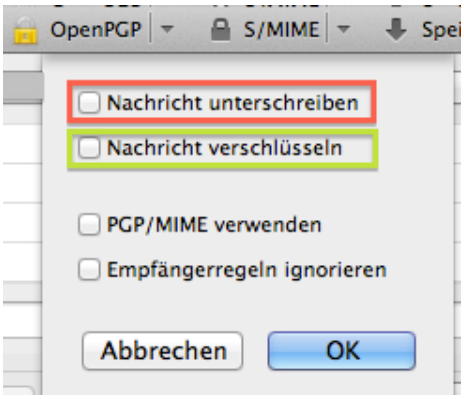

Abbildung 6: Digitale Signatur und Verschlüsselung mittels PGP in Thunderbird

Jetzt nur noch auf „Senden“ drücken und fertig ist der Versand einer verschlüsselten und/oder signierte Email.

Trotz sorgfältiger inhaltlicher Kontrolle übernimmt das ISDSG keine Haftung auf Richtigkeit, Vollständigkeit und Aktualität dieses Dokumentes.

Für weitere Fragen und Anregungen stehen wir Ihnen gerne zur Verfügung.

ISDSG – Institut für Sicherheit und Datenschutz im Gesundheitswesen
c/o Jäschke Health Care Consulting
Westfalendamm 251
44141 Dortmund

Fon. +49 231 449949991
Fax. +49 231 449949999
M@il kontakt@isdsg.de
www https://www.isdsg.de

Trotz sorgfältiger inhaltlicher Kontrolle übernimmt das ISDSG keine Haftung auf Richtigkeit, Vollständigkeit und Aktualität dieses Dokumentes.

Für weitere Fragen und Anregungen stehen wir Ihnen gerne zur Verfügung.

ISDSG – Institut für Sicherheit und Datenschutz im Gesundheitswesen
c/o Jäschke Health Care Consulting
Westfalendamm 251
44141 Dortmund

Fon. +49 231 449949991
Fax. +49 231 449949999
M@il kontakt@isdsg.de
www https://www.isdsg.de